DoD Certificate Policies

Federal PKI Technical Working Group

13 May 1999

Dave Fillingham
dwfilli@missi.ncsc.mil

Overview

- What is a certificate policy?
- How the DoD certificate policies will be used
- Influences on the DoD certificate policies
- DoD certificate policy highlights
- Policy management and enforcement
- Status - and how you can comment
- Summary and conclusions

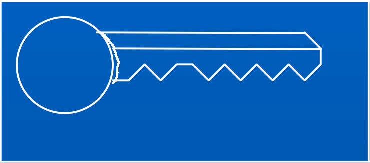
What is a Certificate Policy?

- **Defined by ISO/ITU X.509**

“A named set of rules that indicates the applicability of a certificate to a particular community **and/or class of application with** common security requirements.”

- **Minimize references to implementation**
- **Based on certificate issuance requirements, certificate use, or other community aspect**
- **Roughly speaking - a “certificate policy” describes the** “level of assurance” **one can ascribe to a certificate asserting the policy, and the** community **and** applications **the certificates are intended to be used for.**

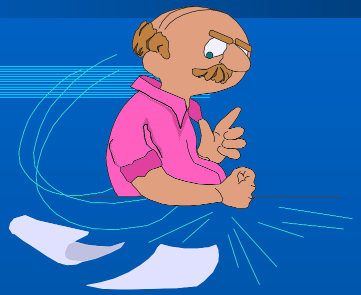
Certificate Policies Asserted in Certificates

Name		Policy OID: (2)(16)(840)...	Signature

- Object Identifiers (a series of integers) asserted in certificates by Certification Authority (CA)
- **Assertion of a policy OID in a certificate represents a promise by the CA that the certificate was generated in accordance with the stipulations of the policy!**
- **Relying parties (those using a certificate to verify a signature) can choose a certificate to be acceptable or not based on an “Acceptable Policy Set” (X.509 Standard)**
- Today, most applications ignore noncritical policies.

Who’s Impacted by Certificate Policies?

Legal Experts



Policy Developers

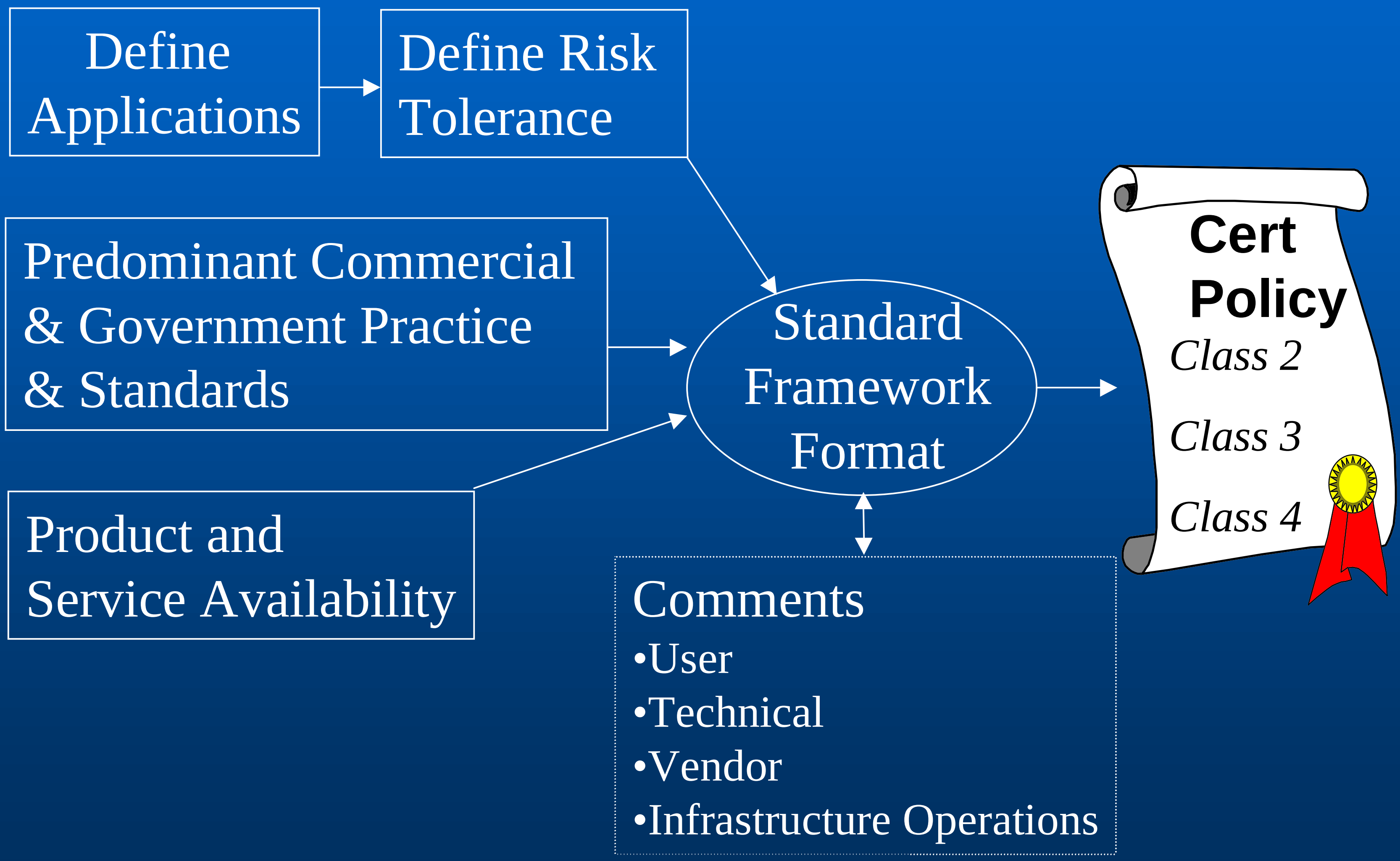
Cost Analysts

Certification Authorities (Internal and External)

Certificate Infrastructure Component & Application Developers

End Users (Subscribers and Relying Parties)

DoD Approach to Policy Development



Define Applications

Define Risk Tolerance

Predominant Commercial & Government Practice & Standards

Product and Service Availability

Standard Framework Format

Comments
- User
- Technical
- Vendor
- Infrastructure Operations

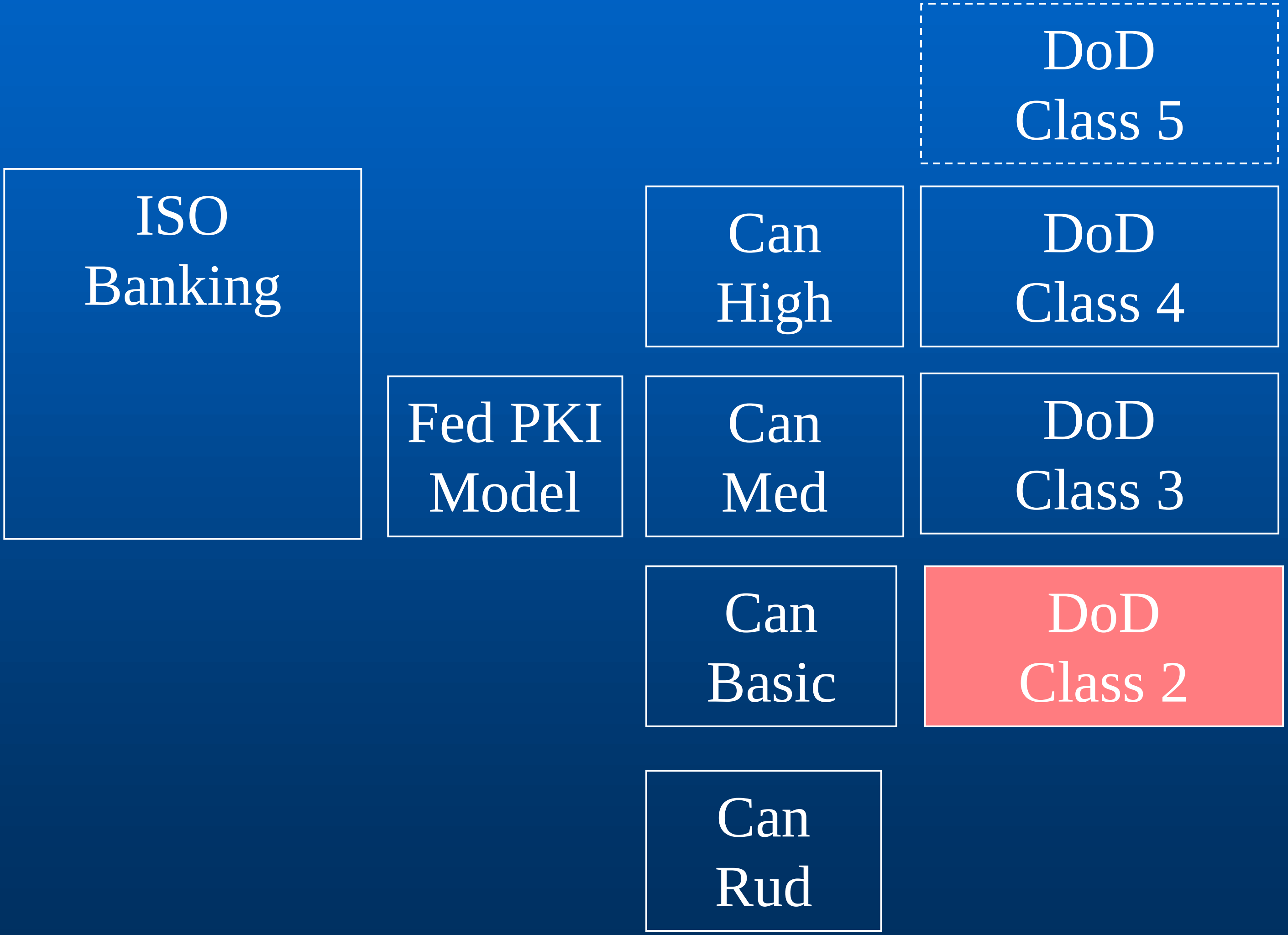
Cert Policy

Class 2

Class 3

Class 4

Rough Equivalencies Between Policies



DoD Class 5

ISO Banking

Can High

DoD Class 4

Fed PKI Model

Can Med

DoD Class 3

Can Basic

DoD Class 2

Can Rud

Applicability

- CLASS 2:
  - Digital signature for mission support/administrative
  - Key exchange for privacy of system high on encrypted network, or low value info on unencrypted network
  - Small value financial transactions (travel claims, credit card)
- CLASS 3:
  - Digital signature for mission critical and national security info on encrypted network
  - Key exchange for protection of COI and low value info on encrypted network
  - Medium value financial transactions (payroll, contracting)
- CLASS 4:
  - Digital signature for unclassified mission critical or national security info on unencrypted network
  - Key exchange for confidentiality of high value compartmented info on encrypted networks
  - Protection of information crossing classification boundaries low to high
  - Large value financial transactions

Identification and Authentication

- CLASS 2:
  - Alternate name form only acceptable*
  - Identity established via database
  - Two re-keys chained off existing certificate
  - Re-key required every five years
- CLASS 3:
  - Alternate name form only acceptable (with restrictions)*
  - Identity established in person (via notary acceptable)
  - Two re-keys chained off existing certificate
  - Re-key required every three years
- CLASS 4:
  - DN required
  - Identity established in person (to RA)
  - No chained re-keys
  - Re-key required every three years

* CA, RA always require DN

Operational Requirements

- CLASS 2:
  - **No CRL periodicity required**
  - **Compromise CRL within 24 hr of notification**
  - **Archive for seven years, six months**
  - **CA key/certificate life 10/5 years**
- CLASS 3:
  - **CRL periodicity weekly**
  - **Compromise CRL within 24 hr of notification**
  - **Archive for ten years, six months**
  - **CA key/certificate life 6/3 years**
- CLASS 4:
  - **CRL periodicity daily**
  - **Compromise CRL within 6 hr of notification**
  - **Archive for twenty years, six months**
  - **CA key/certificate life 6/3 years**

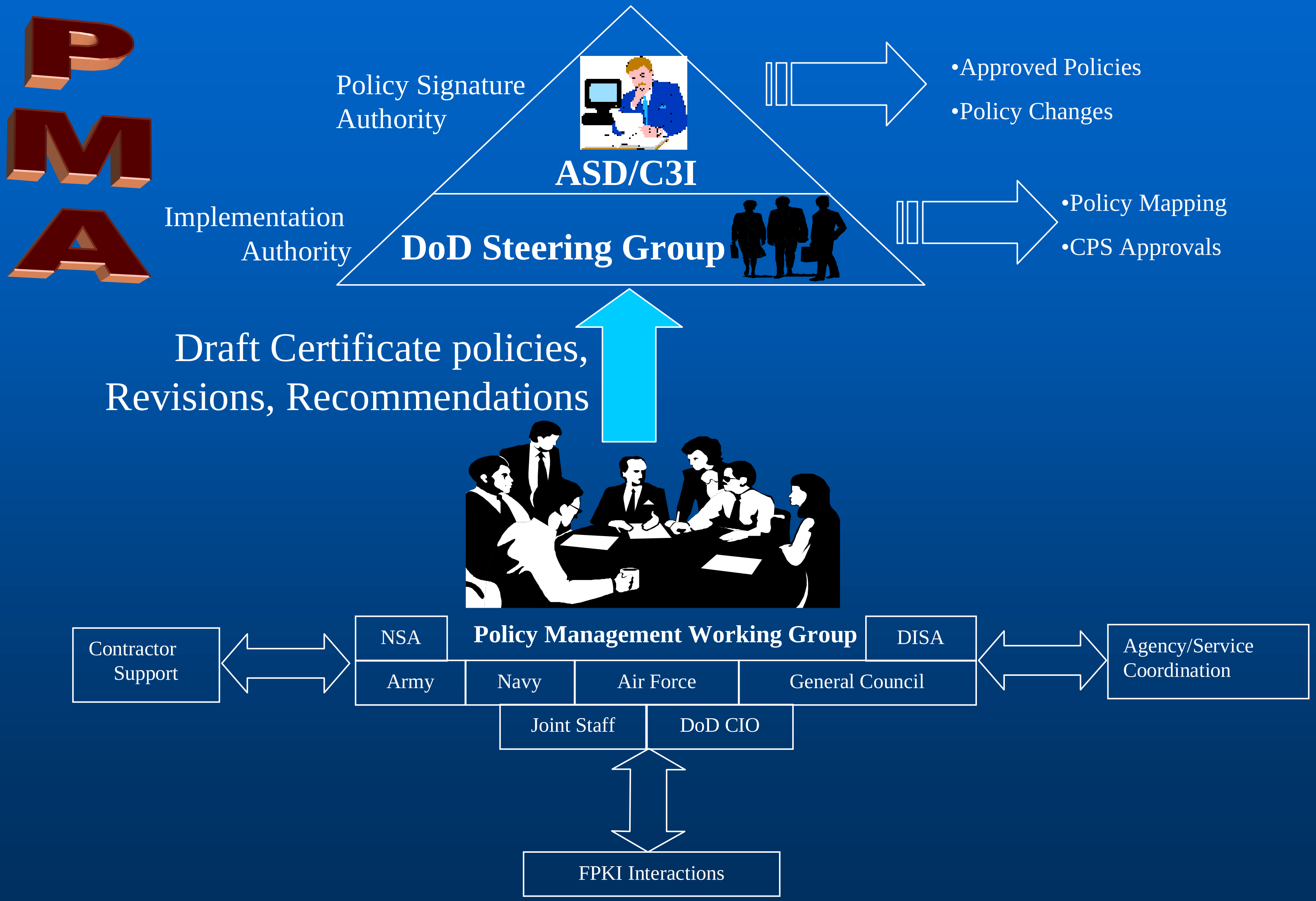
Technical Security Controls

- CLASS 2:
  - **End user token FIPS 140-1 Level 1**
  - **CA token FIPS 140-1 Level 2 (HW or SW)**
  - **C2 or E2/F-C2 evaluated CA platform**
  - **Random package selection**
- CLASS 3:
  - **End user token FIPS 140-1 Level 1**
  - **CA token FIPS 140-1 Level 2 (HW)**
  - **C2 or E2/F-C2 evaluated CA platform**
  - **Tamper-evident packing or hand carry**
- CLASS 4:
  - **End user token FIPS 140-1 Level 2**
  - **CA token FIPS 140-1 Level 2 (HW)**
  - **Design to: B1 platform, TSDM Level 2 application**
  - **Tamper-evident packing or hand carry**

Certificate Profile

- CLASS 2:
  - **Governed by FPKI profile**
  - **RSA or DSA or KEA algorithms**
  - **No name and path length constraints**
- CLASS 3:
  - **Governed by FPKI profile**
  - **RSA or DSA, KEA algorithms**
  - **No name and path length constraints**
- CLASS 4:
  - **Governed by SDN.706**
  - **DSA, KEA algorithms (requirement implied)**
  - **Name and path length constraints**

DoD PMA Approach



PMA

Policy Signature Authority

ASD/C3I

- Approved Policies
- Policy Changes

Implementation Authority

DoD Steering Group

- Policy Mapping
- CPS Approvals

Draft Certificate policies, Revisions, Recommendations

Contractor Support

Policy Management Working Group

NSA

DISA

Army

Navy

Air Force

General Council

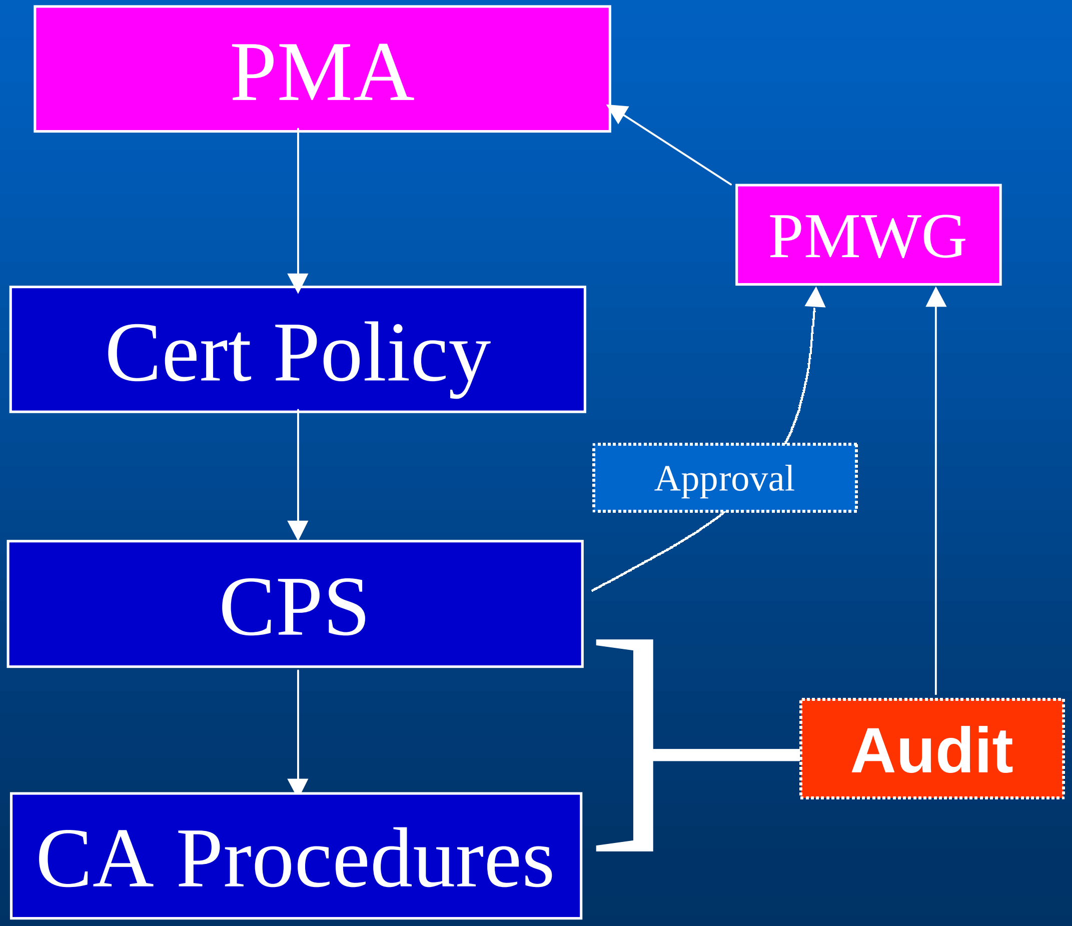
Joint Staff

DoD CIO

Agency/Service Coordination

FPKI Interactions

Certificate Policy Enforcement Chain



Policy Plans

- Latest draft released from ASD/C3I to all of DoD and to 25 companies on 28 April 1999
- Comments due 2 July 1999
- Anticipate ASD/C3I sign-out 31 July 1999
- You are welcome to send comments to:

Karen Gorsuch/Joe Mirabile
OASD(C3I)/IA, 6000 Defense Pentagon, Room 3D239,
Washington, DC 20301-6000
FAX: (703) 614-7484 Phone: (703) 697-5936

Summary and Conclusions

- DoD Certificate Policy has to balance security and cost.
- Policy equally applicable to insourced, outsourced, centralized and distributed CAs.
- Class 2 certificate policy not planned to be implemented
- Class 3 certificate policy likely to predominate at first.
- Class 4 certificate policy initially used for organizational military messaging
- DoD PKI Roadmap calls for Class 4 to eventually supplant Class 3